

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA**

Alexandria Division

UNITED STATES

v.

ROHIT JAWA,

Defendant.

Case No. 1:15-MJ-332

UNDER SEAL

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

I, John Watson, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of a criminal complaint charging ROHIT JAWA with violations of 18 U.S.C. §1028.
2. I am a Special Agent with the United States Postal Service Office of Inspector General (USPS OIG) and have been so employed since May 2011. Prior to that, I was a Special Agent with the Naval Criminal Investigative Service for two years and with the Air Force Office of Special Investigations for three years. I am a graduate of the Criminal Investigator Training Program at the Federal Law Enforcement Training Center in Glynco, GA and have received formal training in the investigation of computer crimes, including network intrusions and access device fraud, from the Defense Cyber Investigations Training Academy in Linthicum, MD. I have a bachelor's degree in Business Administration from The College of Charleston, South Carolina. I have investigated or assisted in the investigation of a number of cases involving

fraudulent activity in connection with computers. I am currently assigned to the Postal Service OIG's Computer Crimes Unit and investigate or assist in the investigations of violations of federal laws regarding property in the custody of the Postal Service, property of the Postal Service, the use of the mails, and other postal offenses, including the impersonation of Postal Service employees. I have received extensive specialized training in these fields. I have been a sworn law enforcement officer during all times herein.

3. This affidavit is intended to show merely that there is probable cause Rohit Jawa has committed the aforementioned violations and does not set forth all of my knowledge about this matter. The information in this affidavit comes from my personal knowledge and information other individuals have provided to me.

PROBABLE CAUSE

Background on Involved Entities

4. The Postal Reorganization Act of 1970 established the Postal Service as an independent establishment within the executive branch of the Government of the United States, pursuant to 39 U.S.C. § 201. Pursuant to 39 U.S.C. § 101, the Postal Service's primary purpose is to provide postal services facilitating interstate commerce and communication. Public Law 104-208 established an Office of Inspector General for the Postal Service. The Postal Service Office of Inspector General (USPS OIG) headquarters are in Arlington, VA, in the Eastern District of Virginia. In addition to the authorities granted by the Inspector General Act, the Postal Service Board of Governors has designated USPS OIG Special Agents as agents authorized to exercise the Postal Service's investigative and law enforcement authorities, pursuant to 18 U.S.C. § 3061.

5. The Federal Bureau of Investigation (FBI) is an agency within the U.S. Department of Justice, an executive department of the United States, pursuant to 28 U.S.C. § 531 and 5 U.S.C. § 101. The FBI operates a service, formerly known as “Law Enforcement Online” and now known as the “Law Enforcement Enterprise Portal” (LEO) which provides authorized law enforcement officers an email account in the “leo.gov” domain and single-sign on access to multiple sensitive U.S. government computer systems. All FBI computer systems referenced in this affidavit are protected computers within the definition at 18 U.S.C. § 1030(e)(2), as they are for the exclusive use of the United States Government and its authorized users. The LEO sign-in page contains a conspicuous notice advising visitors they are accessing a U.S. government information system provided for U.S. government-authorized use only.

6. LocatePLUS is a Massachusetts corporation providing, according to their published privacy policy, a database of “nonpublic and public information to carefully screened and certified entities who are legally qualified to receive this information under the Gramm-Leach-Bliley Act [Public Law 106-102], the Drivers Privacy Protection Act [18 U.S.C. § 2721 et seq.], and the Fair Credit Reporting Act [15 U.S.C. § 1681 et seq.], among other applicable state and federal laws.” This database contains information such as names, email addresses, Social Security Numbers, birth dates, current and historical addresses and phone numbers, driver license and motor vehicle records, tax assessment and land ownership records, and civil, criminal, and bankruptcy court records. This includes information constituting of a “means of identification” within the definition at 18 U.S.C. § 1028(d)(7) . LP Police is a division of LocatePLUS that provides these services to users from verified law enforcement and government agencies. LocatePLUS and LP Police computer systems are protected computers within the

definition at 18 U.S.C. § 1030(e)(2), as they are used in and affect interstate commerce and communication.

7. eBay is an online marketplace that allows users to sell items to other users.

8. PayPal is an online funds transfer and payment service. Users can send and receive funds from other users and transfer funds to and from their PayPal account from other financial instruments, including bank accounts and credit cards. During the majority of the time period covered in this affidavit, PayPal was the primary payment mechanism for eBay sales. PayPal requires users to provide information constituting of a "means of identification" within the definition at 18 U.S.C. § 1028(d)(7) to register for an account.

9. eBay's ShipCover program offers sellers the option to add insurance through a third-party insurance company when printing a shipping label to ship an item they have sold to a buyer. In the event the Postal Service loses or damages an insured package, the insurance company pays the claim to the seller's PayPal account.

eBay/PayPal & Insurance Fraud Scheme

10. Since January 2013, a set of at least 19 eBay and 18 PayPal accounts have been engaged in a scheme to defraud eBay buyers and eBay's third-party parcel insurance company.

11. In December 2013, the ShipCover program's administrators began investigating a set of accounts which were filing claims on nearly all of their insured parcels. These accounts were linked by overlapping eBay and PayPal accounts and identity information.

12. Insurance company investigators interviewed three people in person whose identities had been used to open these accounts. All three provided insurance company investigators recorded statements denying opening or having any knowledge of the eBay or PayPal accounts opened in their names. In subsequent email conversations with the insurance

program's administrator, the owner(s) of the fraudulent eBay accounts had no knowledge of these in-person interviews. USPS OIG agents subsequently interviewed three others whose identities had been used to open eBay and PayPal accounts; all three denied knowledge of the accounts and stated they had been opened without their knowledge or consent.

13. These accounts used two sets of email addresses in their registration information. The first set was a group of Yahoo accounts ("YAHOO ACCOUNTS") with similarly formatted email addresses; these addresses used a consistent prefix – either "rbox009," "tohaven," or "twaron,"– followed by a hyphen and a varying suffix, for example, "rbox009-cd@yahoo.com" or "tohaven-rn@yahoo.com." The second set were part of 91 email addresses ("1&1 ADDRESSES") that were subordinate to three accounts ("1&1 ACCOUNTS") hosted by 1&1 Mail and Media Inc.; this provider permits users to register numerous addresses under a single account.

14. On May 12, 2015, agents obtained a search warrant from the U.S. District Court for the Eastern District of Virginia for the 1&1 ACCOUNTS.

15. In reviewing the contents of the 1&1 ADDRESSES, agents identified additional eBay and PayPal accounts, beyond those the insurance company identified, that were part of the same pattern of fraudulent activity.

16. Agents located numerous conversations where buyers reported to the seller that they had not received a purchased item, despite Postal Service tracking history showing the item had been delivered. In the case of insured parcels, the seller would often eventually file a claim with eBay's third-party insurance company, using the tracking history as evidence the Postal Service had lost the parcel or it had been stolen. In the case of uninsured parcels, the seller would

use the tracking history to prove to eBay he had shipped the purchased item to the buyer, causing eBay to decide disputes in his favor.

17. Agents found numerous messages in these accounts containing Postal Service tracking numbers for parcels the seller had sent, supposedly using eBay-generated Postal Service shipping labels, but which the buyer claimed to have never received, despite Postal Service tracking history showing the parcel had been delivered. Agents compared destination addresses eBay provided to the Postal Service at the time of the labels' purchase with the addresses seen on the labels when the respective parcels were processed by the Postal Service's mail processing equipment. The addresses on the parcels had been changed from the eBay provided address to different addresses, unaffiliated with the buyer, in the same ZIP code. In my training and experience, this kind of manipulation of a shipping label is a strong indication of fraud.

18. Postal Service tracking information available to customers -- including eBay/PayPal and insurance company personnel -- only displays the five-digit ZIP code where a package was delivered; the delivery location listed is the same for any address within the same ZIP code. Changing the address on the shipping label to a different address in the same ZIP code creates a tracking history that makes it appear as if the Postal Service has delivered the package to the expected destination, rather than an unrelated address within the same ZIP code. A seller can then use this legitimate-looking tracking history to convince eBay, a buyer, or an insurance company that he sent the purchased item to the buyer, when he actually mailed an empty box to a random address in the same ZIP code to generate tracking history. Based on the foregoing information, the relationship between all accounts involved, and discussions with officers who have investigated similar schemes, there is probable cause to believe the seller(s) for this set of

eBay accounts were engaged in such a scheme to generate misleading tracking histories in support of their fraudulent insurance claims and to rebut eBay disputes brought by buyers.

19. These activities constitute a scheme or artifice to defraud. The use of the mail, Internet, and means of identification of multiple people in furtherance of this scheme constitutes violations of 18 U.S.C. §§ 1341, 1343, 1028, and 1028A, respectively.

Impersonation of a USPS OIG agent

20. On July 14, 2014, a buyer who had fallen victim to the previously described fraud scheme complained to the Postal Service about his missing parcel. His complaint eventually reached a USPS OIG special agent, who began investigating the complaint as potential incident of mail theft by a Postal Service employee.

21. On August 7, 2014, the USPS OIG agent corresponded via email with the seller for this transaction at one of the 1&1 ADDRESSES to obtain additional information about the missing parcel. In these emails, the seller requested the USPS OIG agent provide him a copy of his credentials as verification of his identity, which the USPS OIG agent did.

22. On August 9, 2014, the FBI received an application, via the LEO website, for a LEO account, using the USPS OIG agent's identity and a secondary email address that was one of the 1&1 ADDRESSES. The LEO application requires the submission of information constituting of a "means of identification" within the definition at 18 U.S.C. § 1028(d)(7). On August 12, 2014, a person purporting to be this USPS OIG agent contacted FBI technical support personnel by telephone and obtained a temporary username and password for this account. However, in the course of this investigation, the USPS OIG agent advised investigators he never submitted this application or placed this call.

23. Shortly thereafter, an unknown individual used the associated "leo.gov" email account -- a service the FBI provides as part of all LEO accounts -- and a photograph of the USPS OIG agent's credentials obtained during the agent's conversation with the eBay seller, described above, to correspond with LP Police via their website and email seeking an account for their services. He also corresponded with five additional providers of similar services seeking access, but ultimately was not able to gain access to any of these additional services.

24. LP Police, convinced this person was indeed a USPS OIG agent by the fraudulently-obtained "leo.gov" email address and unlawfully-possessed credentials photograph, granted him access to LP Police's systems. Multiple federal and state statutes, and their implementing regulations, restrict access to certain data sets to users in certain roles carrying out specifically enumerated functions. By fraudulently representing himself to LP Police as a USPS OIG agent, this person gained access to data sets he was not authorized to access.

25. On September 4 and 5, 2014, this person accessed LP Police's computer systems using the fraudulently obtained account and obtained sensitive personal information, including information constituting means of identification within the definition at 18 U.S.C. § 1028(d)(7), for at least nine people, including the USPS OIG agent whose identity was used to establish the account. The information that individual obtained from LP Police's systems would have been sufficient to facilitate opening eBay, PayPal, and financial accounts using these identities, as LP Police's systems contain answers to many, if not all, of the questions a financial services company might use to verify an applicant's identity.

26. From interviewing the people whose information was queried, and reviewing PayPal records and the contents of the 1&1 ADDRESSES, agents determined several of these people, including the impersonated USPS OIG agent, had fraudulent eBay, PayPal, and other

financial accounts opened using their identities, without their knowledge or consent. These accounts were registered using addresses in the 1&1 ADDRESSES block.

Attribution

27. I submit there is probable cause to believe ROHIT JAWA was the individual who carried out all of the previously-described violations for the following reasons:

28. First, there is a distinct pattern that all identifiable IP addresses used to access the fraudulent eBay, PayPal, financial, 1&1 ACCOUNTS, LEO account, and other involved accounts are IP addresses at JAWA's residences and employers.¹ As JAWA moves to a new residence or job, the IP addresses observed also move to those at the new employer or residence. This pattern exists for the duration of the scheme, from approximately 2013 through the present, across at least five employers and three residence locations.

29. Second, all three of the 1&1 ACCOUNTS were being accessed contemporaneously from the same IP addresses, indicating they are under the control of the same person or persons. The most recent activity in the 1&1 ACCOUNTS came from an IP address that the service provider, Cincinnati Bell, advised has been assigned to JAWA since March 3, 2015, with service provided at an address in Cincinnati, OH where JAWA is currently receiving mail. In a potentially unrelated matter, JAWA contacted USPS OIG twice using his actual identity for assistance with mail delivery service issues and provided his personal email address,

¹ The user at times relied on anonymization services or cellular internet connections to mask his IP identity. However, there are regular instances where the user failed to adequately or completely anonymize his identity. Most of these trace to an address associated with JAWA. For example, beginning in 2013, IP addresses associated with the Mississippi Educational Network are observed accessing the fraudulent eBay and Paypal accounts. This corresponds to the time that JAWA was a student at Alcorn State University in Lorman, Mississippi. In September 2014, IP addresses accessing the fraudulently created LEO account trace back to a residence where JAWA was then a renter. In December 2014, IP addresses accessing these accounts trace to Kaiser Permanente, where JAWA was then a subcontractor. From late 2014 through early 2015, IP addresses accessing these accounts trace to a Denver, Colorado, residence where JAWA was then a renter. In May 2015, IP addresses accessing these accounts trace to Kroger Company, where JAWA was working as a subcontractor. During the same time frame, IP addresses accessing these accounts, as well as JAWA's personal email account, traced to JAWA's residence.

esifts@gmail.com, as contact information. The U.S. District Court for the Eastern District of Virginia authorized the installation of a pen register/trap and trace (pen/trap) device on this account. Data from the pen/trap device indicates JAWA is currently accessing his personal email account from this IP address.

30. Third, two companies at which JAWA has worked as a contractor, including the company where he currently works, advised investigators that activity observed in this scheme from their IP addresses came from computers, IP address, or accounts assigned to JAWA.

31. Fourth, many of the identities used for the fraudulent eBay, PayPal, financial, email, and other accounts have a connection to JAWA; they are people with whom he has lived or who attended his university, Alcorn State University in Lorman, MS.

32. Fifth, some of the initial eBay activity occurred using eBay accounts registered using JAWA's own name and a username that is the same as the username on his personal email address.

33. The YAHOO ACCOUNTS use distinctly-formatted addresses; these addresses used a common prefix – either “rbox009,” “tohaven,” or “twaron” – followed by a hyphen and a varying suffix, for example, “rbox009-cd@yahoo.com” or “tohaven-rn@yahoo.com.” These sets of addresses are connected to each other and the 1&1 ADDRESSES by overlapping use of PayPal accounts for transactions and stolen identities used in registration information. I submit this indicates the YAHOO ACCOUNTS and 1&1 ACCOUNTS are under the control of the same person or persons, and as there is probable cause to believe JAWA controls the 1&1 ACCOUNTS, there is probable cause to believe he also controls the YAHOO ACCOUNTS. By extension, there is also probable cause to believe he controls the eBay, PayPal, and financial

accounts registered using either the YAHOO ACCOUNTS or the 1&1 ADDRESSES, which includes all accounts of this nature described in this affidavit.

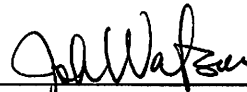
34. JAWA also uses this same format of email address as the YAHOO ACCOUNTS, including the "rbox009" prefix, in some of his personal accounts. According to records LinkedIn produced in response to a subpoena, JAWA's personal account on LinkedIn – a business-oriented social networking site and digital resume system – has three associated email accounts, two of which, rbox009-android@yahoo.com, and rbox009-mail@yahoo.com, use an identical format and prefix.

35. Finally, Citibank investigators advised that numerous credit card numbers connected to several of the fraudulent PayPal accounts were part of a Citibank account in JAWA's name.

Conclusion


36. Based on the foregoing, I submit there is probable cause that ROHIT JAWA has violated 18 U.S.C. § 1028, and I respectfully request the court issue a warrant for his arrest.

Respectfully submitted,



John Watson
Special Agent
United States Postal Service
Office of Inspector General

Subscribed and sworn to before me on June 15, 2015

_____/s/ 
Michael S. Nachmanoff
United States Magistrate Judge

Honorable Michael S. Nachmanoff
UNITED STATES MAGISTRATE JUDGE